IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, February 2026
Impact Factor: 8.2

Robust Intrusion Detection System for Military Wireless Sensor Networks Applications

Sumedh Dhengre[1], Upeksha Kohak[2], Rajnandini Patil[3], Sagar Swami[4], Ayush Suryavanshi[5]
Guide, Department of Computer Engineering[1]
Students, Department of Computer Engineering[2,3,4,5]
AISSMS COE, Pune, Maharashtra

Abstract: *Wireless Sensor Networks (WSNs) play a crucial role in modern military communication and surveillance but are increasingly vulnerable to cyberattacks due to their distributed and resource-constrained nature. Traditional security measures such as encryption and firewalls are insufficient for real-time threat detection in these environments. This research aims to design a lightweight Intrusion Detection System (IDS) using machine learning algorithms—Decision Tree, Random Forest, and KNearest Neighbors (KNN)—to identify malicious network traffic effectively. The system's methodology involves dataset preprocessing, model training, and performance evaluation using benchmark datasets such as UNSW-NB15 and CIC-IDS2017. Preliminary analysis suggests that ensemble-based models like Random Forest can achieve high detection accuracy (around 98%) with minimal computational cost. The significance of this work lies in its potential to provide a reliable, energy-efficient, and real-time security framework for military WSN applications. This paper represents the design and planning phase, with implementation and testing to be carried out in the next phase*

Keywords*:* Intrusion Detection, Wireless Sensor Network, Machine Learning, Cybersecurity, Military Applications, Decision Tree, Random Forest, KNN

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are collections of small, low-power sensor nodes capable of sensing, processing, and communicating data wirelessly. They play a crucial role in defense and military operations such as border surveillance, battlefield monitoring, and secure communication systems. These networks enable real-time situational awareness and decision-making in critical scenarios.

However, due to their distributed nature and limited processing, energy, and memory resources, WSNs are highly vulnerable to a range of cyber threats. Attackers can exploit weaknesses to disrupt communication, alter sensed data, or even disable the entire network. The consequences of such intrusions in military systems can be severe, leading to compromised missions or loss of critical intelligence.

Traditional security mechanisms such as encryption, firewalls, or authentication are often insufficient in these constrained environments. They require higher computational power and battery resources, making them unsuitable for real-time detection in largescale sensor deployments. This motivates the need for a lightweight, intelligent Intrusion Detection System (IDS) that can detect anomalies quickly and accurately while consuming minimal resources.

The scope of this research focuses on the design and analysis phase of a machinelearning-based IDS for military WSNs. The implementation and experimental evaluation will be conducted in the next project phase.

The objective of this study is to develop a framework using Decision Tree, Random Forest, and K-Nearest Neighbors (KNN) algorithms to detect intrusions efficiently, ensuring high accuracy, low computational complexity, and adaptability for real-time military operations.

DOI: 10.48175/IJARSCT-31157

II. PROBLEM STATEMENT

Despite the advances in network security, existing Intrusion Detection Systems for Wireless Sensor Networks suffer from high computational costs and limited adaptability to dynamic environments. There is a lack of lightweight, real-time IDS solutions specifically optimized for military-grade WSNs.

The proposed solution aims to achieve an optimal balance between detection accuracy and computational cost, making it suitable for real-time military operations.

III. LITERATURE REVIEW

Several researchers have explored machine learning and deep learning techniques to enhance intrusion detection in Wireless Sensor Networks (WSNs).

o Talukder et al. (2024) proposed a hybrid model combining Random Oversampling (RO), Stacking Feature Embedding (SFE), and Principal Component Analysis (PCA) to handle data imbalance. Their approach achieved above 99% accuracy but required significant computational resources, making it unsuitable for resourcelimited WSNs.

o Kasongo and Sun (2020) introduced a deep learning method using wrapper-based feature extraction for intrusion detection. Although it achieved high detection performance, the model required long training time and powerful hardware, limiting its use in real-time military scenarios.

o Ahmad et al. (2023) suggested a Random Forest-based model for efficient attack detection and demonstrated that ensemble methods can deliver strong performance while being relatively lightweight. However, their work did not address the optimization of IDS for extremely resource-constrained sensor nodes.

Comparison and gap Analysis:

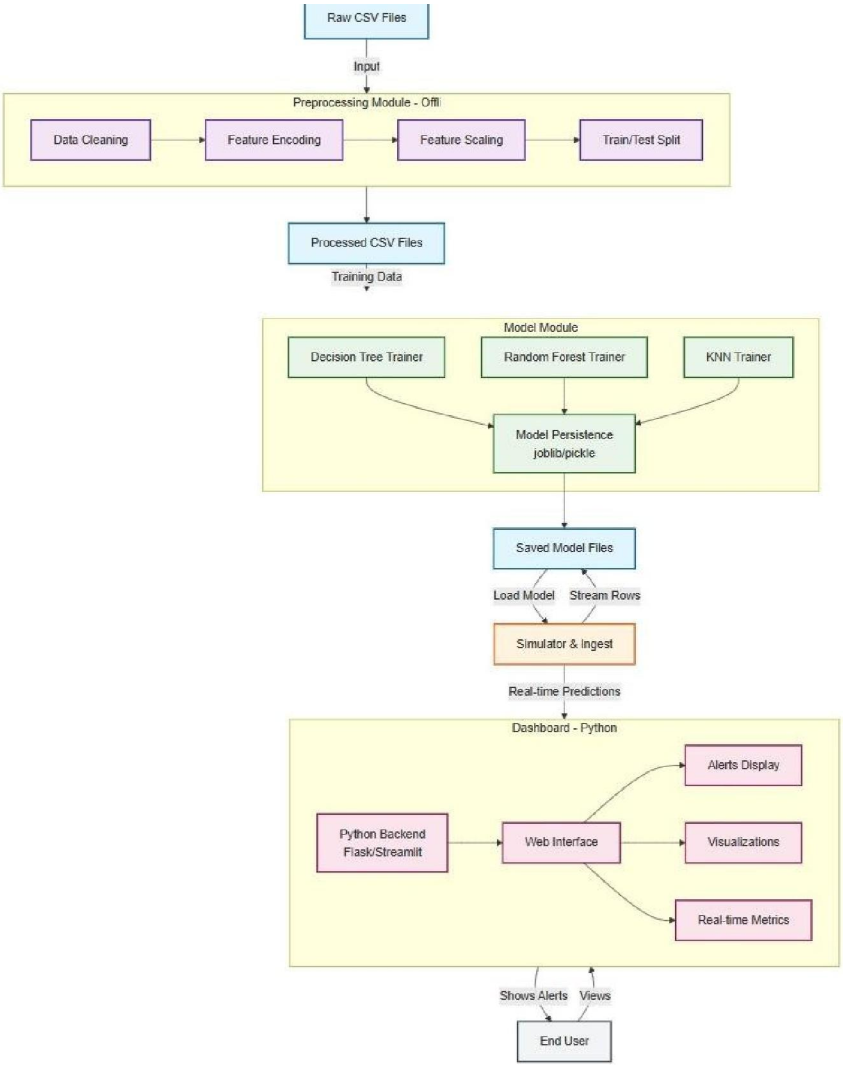
From the above studies, it is evident that deep learning models provide excellent accuracy but are computationally intensive and energy-demanding. On the other hand, traditional machine learning models like Decision Tree, Random Forest, and KNN offer comparable results with significantly lower complexity. Existing literature lacks an approach specifically optimized for military-grade WSNs, where both accuracy and energy efficiency are equally important.

Proposed Improvement:

The present research addresses this gap by developing a lightweight machine learning- based IDS that combines high detection accuracy with low computational cost. By focusing on interpretable models and optimized preprocessing, the proposed approach aims to make real-time intrusion detection feasible for constrained military environments.

From this literature, it is evident that while deep learning models provide high accuracy, simpler algorithms like Decision Tree, Random Forest, and KNN can still deliver strong performance with much lower computational demand. Therefore, this study focuses on building an IDS using these lightweight machine learning models for military WSN applications.

DOI: 10.48175/IJARSCT-31157



IV. PROPOSED METHODOLOGY

The proposed Intrusion Detection System (IDS) for Wireless Sensor Networks (WSNs) is designed through multiple phases including dataset selection, data preprocessing, model training, testing, and evaluation. The focus is on building lightweight models suitable for real-time deployment in constrained military environments.

4.1 Dataset Selection:

The UNSW-NB15 dataset is selected for model training and evaluation, as it contains a diverse set of modern attack types such as Exploits, DoS, Worms, and Reconnaissance. The CIC-IDS2017 dataset may also be used for validation to test the generalization of the model. These datasets include both normal and abnormal traffic generated through a hybrid of real and synthetic network environments.

4.2 Tools and Technologies Used

The implementation will be carried out using Python (scikit-learn, pandas, NumPy, matplotlib) for machine learning, preprocessing, and visualization. Simulation and testing in real-time WSN conditions will be performed using NS2 or MATLAB in the next development phase.

4.3 Data Preprocessing

Before training, the dataset undergoes the following steps:

- Cleaning: Removing missing or duplicate entries to ensure data integrity.
- Encoding: Converting categorical attributes (e.g., protocol, service, flag) into numerical format using Label Encoding.
- Normalization: Scaling numeric values to a common range to avoid algorithmic bias.
- Splitting: Dividing the dataset into 80% training and 20% testing subsets.

This ensures efficient learning and consistency in evaluation.

4.4 Model Training and Selection

Three machine learning algorithms are trained and compared:

- Decision Tree (DT): Classifies data using feature-based splitting, offering easy interpretability.
- Random Forest (RF): An ensemble of multiple trees to improve accuracy and reduce overfitting.
- K-Nearest Neighbors (KNN): Classifies samples based on proximity to existing data points.

Each model will be trained on the same dataset to ensure fair comparison and evaluated for accuracy, precision, recall, and F1-score.

4.5 Model Evaluation:

Performance metrics include Accuracy, Precision, Recall, F1-Score, and a Confusion Matrix to visualize prediction outcomes. These metrics collectively determine the most efficient algorithm for real-time intrusion detection.

4.6 System Architecture

The overall architecture (Figure 1) includes the following modules:

- Data Collection Module: Captures real-time traffic from WSN nodes.
- Preprocessing Unit: Cleans and formats data for analysis.
- Classification Engine: Uses trained ML models (DT, RF, KNN) for anomaly detection.
- Alert Generation Module: Sends real-time notifications when intrusions are detected.

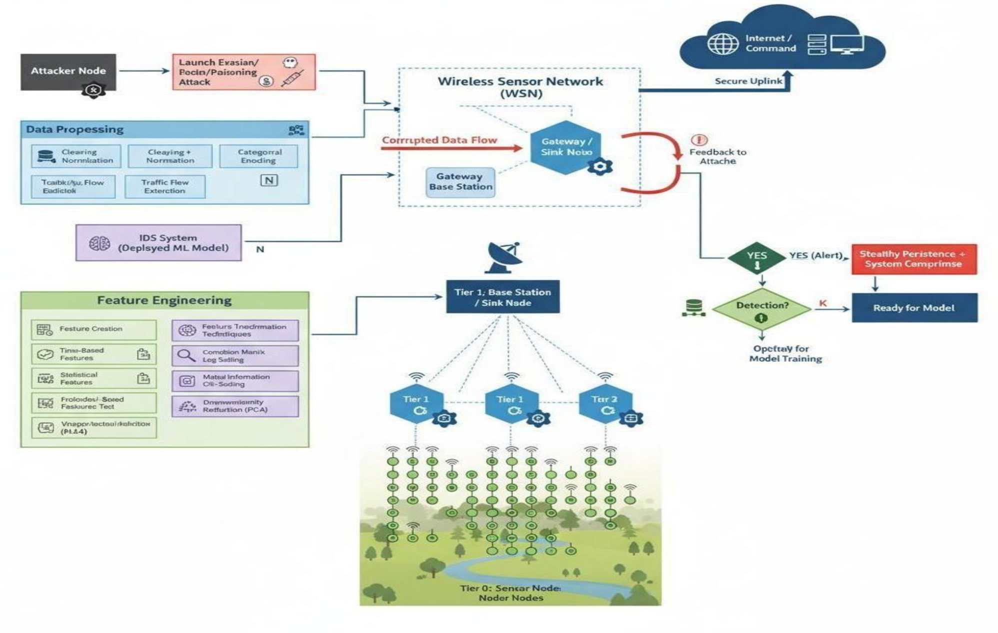

Attacker Node
Launch Exasian/ Pocin/Paisoning Attack
Wireless Sensor Network (WSN)
Internet / Command
Secure Uplink
Data Propessing
Clearing Normlization
Cleaying + Normation
Categorral Enoding
Tcaibk:/şu. Flow Eadictek
Traffic Flew Exterction
N
Corrrıpted Data Flow
Gateway / Sink Neto
Gateway Base Station
Feedback to Attache
IDS System (Deplsyed ML Model)
N
YES
YES (Alert)
Stealthy Peristence + System Cemprimse
Detection?
K
Ready for Model
Opcftaiy for Model Training
Feature Engineering
Festure Crestion
Feelurs Tnedrmation Tedmtiques
Tima-Based Festures
Comobion Manix Leg Salling
Stetistical Features
Matal Infomation Oli-Soding
Frolodes/-Sored Faskurec Tect
Dmmwmisinity Refturtion (PCA)
Vnapor/lectsui/kslicitiox (PI.A4)
Tier 1; Base Station / Sink Nsde
Tier 1
Tier 1
Terr 2
Tier 0: Sencar Node: Noder Nodes

Figure 1: System Architecture of the Proposed Intrusion Detection System.

DOI: 10.48175/IJARSCT-31157

It illustrates the architecture of the proposed Intrusion Detection System (IDS) for Wireless Sensor Networks (WSNs) used in military applications. The architecture shows how network data flows from sensor nodes (Tier 0) through various tiers and the base station (Tier 1) before being processed by the IDS. Data preprocessing, feature engineering, and machine learning models are applied to detect malicious activity. The system identifies attack patterns, generates alerts, and supports real-time threat detection while maintaining low resource usage.

4.7 Workflow:

The step-by-step process is depicted in Figure 2, starting with data acquisition, preprocessing, and model training, followed by testing and evaluation. This systematic approach ensures robust performance and adaptability.

It presents the overall methodology of the proposed IDS model. The process begins with dataset loading and preprocessing, followed by model training and validation. The trained model classifies network traffic as normal or malicious. If an attack is detected, it identifies the type of attack; otherwise, the data passes as normal. This workflow ensures systematic detection, evaluation, and model optimization for effective intrusion prevention.

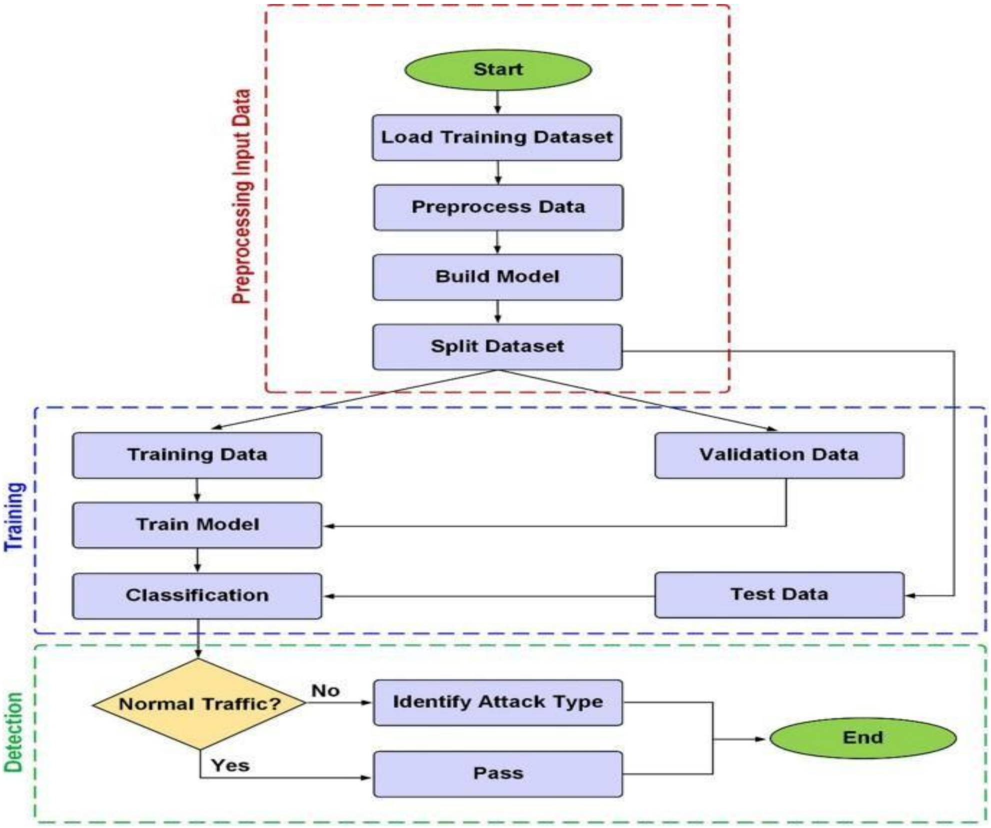


Figure 2: Flowchart of the Intrusion Detection Process.

VII. EXPECTED RESULTS AND FUTURE WORK

The proposed IDS is expected to detect and classify malicious traffic with high accuracy while maintaining low resource usage. Decision Tree and Random Forest are anticipated to outperform KNN in efficiency and interpretability, while KNN may provide better adaptability in dynamic environments.

In the next phase, the models will be implemented using Python (scikit-learn) and tested on benchmark datasets. The system's results will be visualized using performance graphs and confusion matrices. Future enhancements will include integrating deep learning models, feature optimization, and testing the IDS in a simulated WSN environment using tools such as NS2 or MATLAB.

DOI: 10.48175/IJARSCT-31157

VIII. CONCLUSION

This research paper presents a conceptual design of a machine-learning-based Intrusion Detection System for military Wireless Sensor Networks. The study focuses on achieving strong detection accuracy with minimal computational complexity. The approach is intended to provide an efficient, lightweight, and deployable solution for real-time security monitoring in resource-constrained military environments.

The upcoming implementation phase will involve coding, testing, and performance analysis. Comparative results of the three models will be studied to identify the best algorithm for real-world deployment in WSN-based defense applications.

IX. REFERENCES

[1]. Talukder, M. A., Islam, M., Uddin, M. A., et al. “Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding, and feature extraction.” Journal of Big Data, 2024.

[2]. Kasongo, S. M., & Sun, Y. “A deep learning method with wrapper-based feature extraction for wireless intrusion detection.” Computers & Security, 2020.

[3]. Ahmad, I., et al. “Feature clustering and random forest-based IDS model for efficient attack detection.” Journal of Information Security and Applications, 2023.

DOI: 10.48175/IJARSCT-31157